Cyber Incident Response: The Handbook for Counsel



Speakers:

Daniel B. Garrie, Esq., Founder, Law & Forensics; Neutral, JAMS; Adjunct, Harvard

Gwenn Cujdik, Manager - North America Cyber Incident Response Team, AXA XL, a division of AXA

James Blair, Head of Digital/CISO, Todd Energy

(c) 2023 Lexeprint Inc. All Rights Reserved

This Photo by Unknown author is licensed under CC BY-SA

Disclaimer



This is not legal advice, nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, as spoken and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.



Soliciting speakers is strictly prohibited.

(c) 2023 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Founder, Law & Forensics
Neutral, JAMS
Adjunct, Harvard



Gwenn Cujdik
Manager - North America
Cyber Incident Response
Team
AXA XL, a division of AXA



James Blair
Head of Digital/CISO
Todd Energy

(c) 2023 Lexeprint Inc. All Rights Reserved

Agenda

- Cyber Risk Landscape
- Attorney Role in Cyber Risk Management and Incident Response
- Regulatory Guidance and Requirements: SEC & FTC
- Prevention Over Cure: Cyber Risk Assessment

(c) 2023 Lexeprint Inc. All Rights Reserved.



Cyber Risk Landscape

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-ND

What is a data breach?

- A data breach is an incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve Personally Identifiable Information (PII), trade secrets or intellectual property.

*National Research Council, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*

(c) 2022 Lexeprint Inc. All Rights Reserved


This Photo by Unknown Author is licensed under CC BY-ND

Lexeprint PUBLISHING GROUP

What is a cyber attack?

- A cyber-attack can be defined as an intentional malicious act or series of acts that exploit computer systems, networks, or devices through the use of various methods and techniques to gain unauthorized access, disrupt operations, steal or damage data, or extort victims. The objective of a cyber-attack can vary, but it typically involves some form of financial gain, political advantage, or personal vendetta.

**National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"*

(c) 2022 Lexeprint Inc. All Rights Reserved


This Photo by Unknown author is licensed under CC BY-NC-ND.

What is a Critical Infrastructure Breach?

- Critical Infrastructure
  - •Targeting businesses that fall under this umbrella can allow foreign actors to disrupt the state more easily by proxy.
  - •85% of U.S. critical infrastructure is privately operated.
- What is a Critical Infrastructure (CI) breach?
  - •A CI breach refers to a security incident that involves unauthorized access, damage, or disruption to systems, networks, or assets that are essential for the functioning of society and economy.

(c) 2023 Lexeprint Inc. All Rights Reserved.



What are Some Weapons Used by Threat Actors?

- Social Engineering
- Unpatched Vulnerabilities
- Bypassing Security
- Denial of Service Attacks (DoS)
- Group Phishing
- Spear Phishing
- Viruses/Worms
- Trojan Horse
- Zero Day Exploit
- Website Exploit
- Spyware, Malware, Ransomware

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-NC

What is Cybersecurity?

- Cybersecurity is the act of protecting information and communications technology (ICT) systems and their contents.
- A broad and arguably somewhat fuzzy concept, cybersecurity can be a useful term but tends to defy precise definition. It usually refers to one or more of three things:
  - A set of activities and other measures intended to protect—from attack, disruption, or other threats—computers, computer networks, related hardware and devices software and the information they contain and communicate, including software and data, as well as other elements of cyberspace.
  - The state or quality of being protected from such threats.
  - The broad field of endeavor aimed at implementing and improving those activities and quality.

(c) 2022 Lexeprint Inc. All Rights Reserved



Questions to consider when assessing threat of a data breach:

- Threats – Who is attacking?
- Vulnerabilities – What weaknesses can be attacked?
- Impacts – What the attack does – what is the financial damage of any breach?
- Value – What is the value of the data to the business, or does it contain PII?

(c) 2022 Lexeprint Inc. All Rights Reserved



Attorney Role in Cybersecurity Risk Management and Incident Response

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-ND

Potential impacts and possible implications for companies

As cyber-attacks continue to multiply and regulatory scrutiny for cyber risk management becomes more sophisticated, businesses face a number of risks from experiencing cybersecurity incidents:

- Loss of revenue,
- Loss of intellectual property,
- Regulatory risk,
- Reputational risk,
- Legal expenses, and
- Board personal liability.

(c) 2023 Lexeprint Inc. All Rights Reserved



Role of Counsel

- Counsel play a central role in helping companies and their board in mitigating risk, responding to regulatory inquiries, and navigating the complex and evolving landscape of cyber risk management
- Mitigation
  - Assessing legal risks through audits and assessments.
  - Developing policies and procedures.
  - Ensuring compliance with applicable cyber and privacy laws.
  - Collaborate and coordinate with outside counsel.

(c) 2022 Lexeprint Inc. All Rights Reserved


This Photo by Unknown Author is licensed under CC BY-ND

Role of Counsel (cont.)

- Incident response
  - Provide legal guidance on breach notification requirements.
  - Manage relationships with law enforcement agencies.
  - Handle communications with customers and stakeholders.
  - Provide guidance on potential litigation risks.
  - Defend against any legal action that may arise.

(c) 2022 Lexeprint Inc. All Rights Reserved



Advising the Board

- It is important that the general counsel, internal audits and ERM give cybersecurity a high priority.

(c) 2022 Lexeprint Inc. All Rights Reserved



Advising the Board (cont)

- Boards should undertake regular, proactive discussions with these functions to ensure their leaders recognize that cyber risk is dynamic and requires continuous external screening for new forms of threat mitigation.
  - For example, internal audits can no longer focus solely on perimeter defense controls, without consideration of risk-based controls.
  - Likewise, ERM should monitor and screen externally new forms of cyber risks, with the awareness that some cyber risks are more qualitative and difficult to measure.

(c) 2022 Lexeprint Inc. All Rights Reserved



Regulatory Guidance and Requirements: SEC & FTC

(c) 2023 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA-NC



SEC 2020 Cybersecurity and Resiliency Observations

The following guidelines were released by the Office of Compliance Inspections and Examinations:

- **Senior Level Engagement.** Devoting appropriate board and senior leadership attention to setting the strategy of and overseeing the organization's cybersecurity and resiliency programs.
- **Risk Assessment.** Developing and conducting a risk assessment process to identify, manage, and mitigate cyber risks relevant to the organization's business. This includes considering the organization's business model, as part of defining a risk assessment methodology, and working to identify and prioritize potential vulnerabilities, including remote or traveling employees, insider threats, international operations and geopolitical risks, among others.
- **Policies and Procedures.** Adopting and implementing comprehensive written policies and procedures addressing the areas discussed below and identified risks.

(c) 2023 Lexeprint Inc. All Rights Reserved



SEC 2020 Cybersecurity and Resiliency Observations

- **Testing and Monitoring.** Establishing comprehensive testing and monitoring to validate the effectiveness of cybersecurity policies and procedures on a regular and frequent basis. Testing and monitoring can be informed based on cyber threat intelligence.
- **Continuously Evaluating and Adapting to Changes.** Responding promptly to testing and monitoring results by updating policies and procedures to address any gaps or weaknesses and involving board and senior leadership appropriately.
- **Communication.** Establishing internal and external communication policies and procedures to provide timely information to decision makers, customers, employees, other market participants, and regulators as appropriate.

(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown author is licensed under CC BY-NC.

2023 Proposed Cybersecurity Rules

- On March 15, 2023, the SEC published long-anticipated proposed cybersecurity and consumer information protection rules.
- The SEC stated that the proposed amendments would:
  - Address the cybersecurity risks for 'Market Entities,'
  - Enable the U.S. securities markets, which part of the critical infrastructure Financial Services Sector, to mitigate risk from cyber incidents through protective measures.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-NC.

Structure of 2023 Proposed Cybersecurity Rules

- The proposal is threefold:
  - An Amendment to Regulation S-P,
  - Proposed Rule 10, and
  - Amendments to Regulation Systems Compliance and Integrity (SCI).
- In according with its rulemaking process, the public comment periods for the proposals will remain open for 60 days after they are published in the Federal Register.

(c) 2023 Lexeprint Inc. All Rights Reserved.

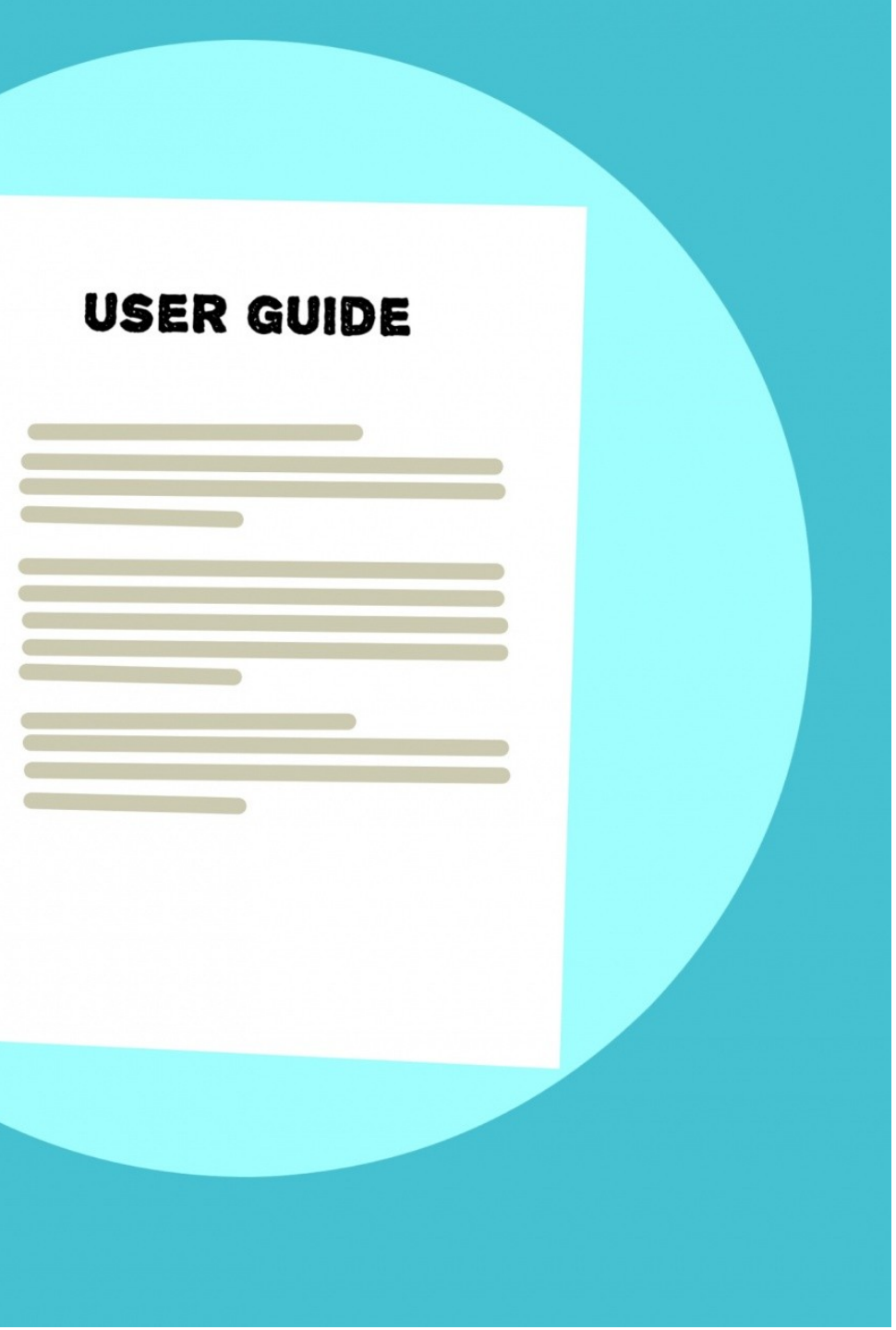


FTC's Health Breach Notification Rule

- The FTC Breach Notification Rule for Electronic Information (16 CFR Part 318) "requires vendors of personal health records and related entities to notify consumers following a breach involving unsecured information."
- Service providers to one of these vendors experiencing a data breach must notify the entity which must then notify consumers.

**Federal Trade Commission, Legal Library*

(c) 2023 Lexeprint Inc. All Rights Reserved.



FTC Data Breach Response Guidance

- The FTC provides the "Data Breach Response: A Guide for Business" in its Business Guidance Resources.
- The key elements of the guidance include
  - Secure operations,
  - Fix vulnerabilities,
  - Notify appropriate parties, and
  - Model letter for informing individuals whose information has been stolen.

(c) 2023 Lexeprint Inc. All Rights Reserved.



Prevention Over Cure: Cyber Risk Assessment

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY

Framework for Cybersecurity

- In 2018, the National Institute of Standards and Technology (NIST) issued a 'Framework for Improving Critical Infrastructure Cybersecurity.' It was written to help improve cybersecurity risk management.
- It can be a guide or model to international cooperations on how to strengthen their cybersecurity in critical infrastructure as well as other sectors and communities.
- The framework consists of three parts: The Framework Core, The Implementation Tiers and the Framework Profiles.

(c) 2023 Lexeprint Inc. All Rights Reserved



What is a cyber risk assessment?

- The NIST defined cyber risk assessments as:
  - "*risks assessments that are used to identify, estimate, and prioritize risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems.*"
- This assessment is used to inform decision-makers and support proper risk responses. It also helps to provide an executive summary to help executives and directors make informed decisions about security.

(c) 2023 Lexeprint Inc. All Rights Reserved


This Photo by Unknown Author is licensed under CC BY-NC-ND

Information Security Risk Assessment

- The information security risk assessment concerns answering the following questions:
  - "What are our organization's most important information technology assets?
  - What data breach would have a major impact on our business whether from malware, cyber attack or human error? Think customer information.
  - What are the relevant threats and the threat sources to our organization?
  - What are the internal and external vulnerabilities?"

**UpGuard*

(c) 2023 Lexeprint Inc. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY

Information Security Risk Assessment (cont.)

Asking the right questions will help you to determine what needs to be protected.

- "What is the impact if those vulnerabilities are exploited?
- What is the likelihood of exploitation?
- What cyber-attacks, cyber threats, or security incidents could impact affect the ability of the business to function?
- What is the level of risk my organization is comfortable taking?"

**UpGuard*

(c) 2023 Lexeprint Inc. All Rights Reserved



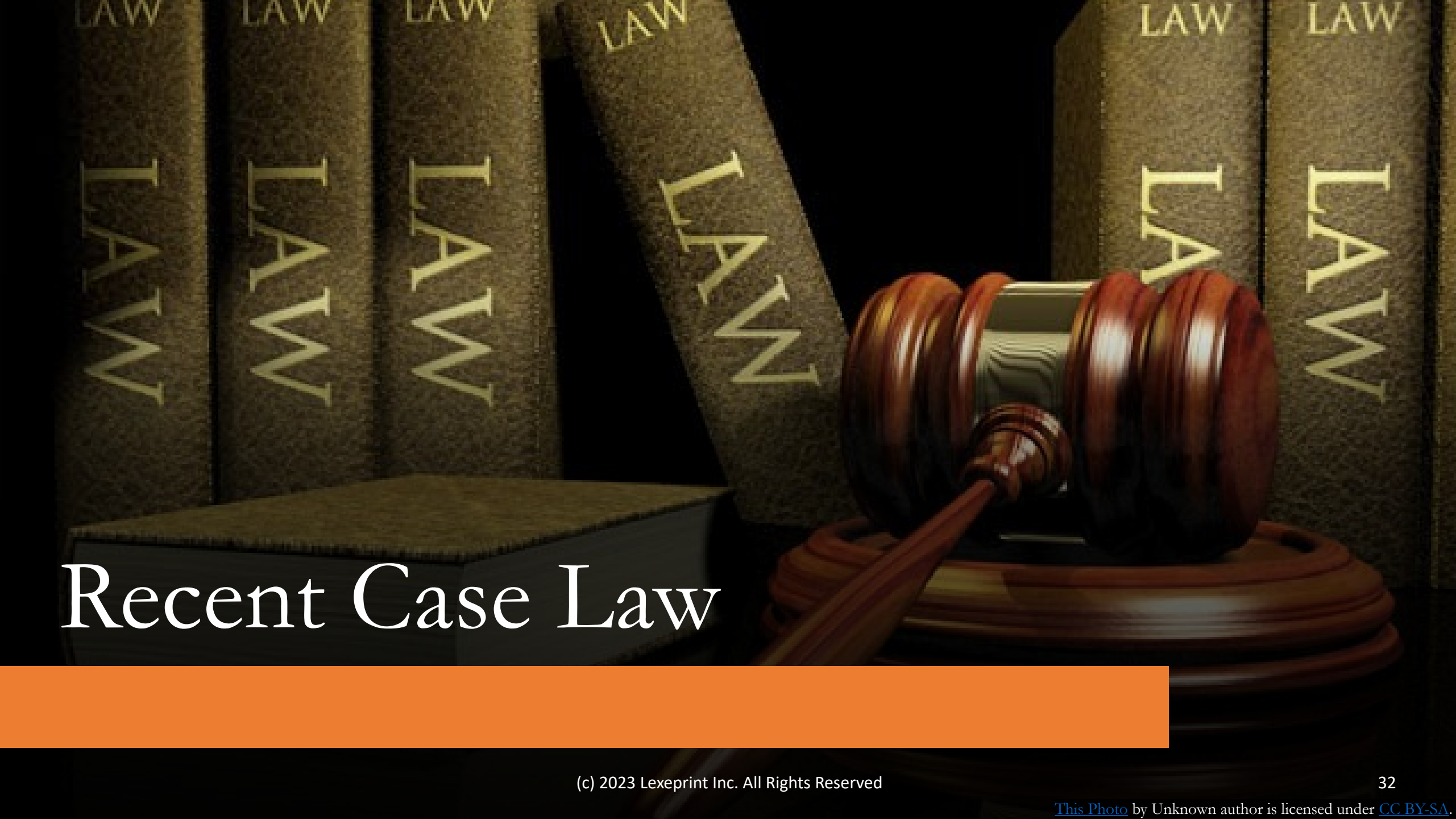
Why You Should Perform Cyber Risk Assessments

Implementing assessment and mitigation solutions that consider both technical risk and leverage regulatory requirements can help lead to:

- Reduction of long-term costs,
- Cyber security risk assessment template for future assessments,
- Avoidance of data breaches,
- Avoidance of regulatory issues,
- Avoidance of data loss.

- Assessments can take the for of audits, workshops or tabletops (simulated cyber event scenarios).
  - Resource: Tabletop.ai

(c) 2023 Lexeprint Inc. All Rights Reserved



Recent Case Law

(c) 2023 Lexeprint Inc. All Rights Reserved

This Photo by Unknown author is licensed under CC BY-SA.


This Photo by Unknown author is licensed under CC BY.

Re: Blackbaud Inc, Customer Breach Litigation, (SC) 2022

Third-party businesses may be liable to parties they do not have direct contact with or a contract.

- **Facts:** Blackbaud is a cloud company that provides data collection and software solutions for non-profit organizations and healthcare entities, among others. The company was hacked, and their client's data, which included the PII of children, was exfiltrated and then held for ransom, which Blackbaud paid in exchange for the commitment that the hackers would destroy the data. The vendor notified its clients months later.
- **Issues:** Did Blackbaud's behavior constitute negligence for not complying with industry and regulatory security standards? Did Blackbaud have a duty to the customers of its clients against the unlawful conduct of a third-party criminal actor?

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown author is licensed under CC BY-SA-NC.

Re: Blackbaud Inc, Customer Breach Litigation, (SC) 2022 (cont.)

- **Ruling:**
  - The court ruled that Blackbaud owed the plaintiffs a duty based off of "Blackbaud's alleged creation of the risk" and the special circumstances of its contracts with Social Good Entities.
  - Following South Caroline law, the court ruled that despite security decisions being made in SC by Blackbaud, injury occurred where the servers were attacked, in Massachusetts. Even though Blackbaud's servers were located across the country, the plaintiffs' data was solely housed in MA.
- **Observations:** Most organizations store data in multiple jurisdictions. Third parties may change the location of their information during the time they are contracted, potentially affecting companies' legal exposure.

(c) 2023 Lexeprint Inc. All Rights Reserved.


This Photo by Unknown Author is licensed under CC BY-ND

Vash v. T-Mobile US, Inc (GA) 2021

- **Facts:** Plaintiff Stephen J. Vash filed a suit seeking compensation for a T-Mobile data breach that compromised the personal data of more than 50 million people. T-Mobile includes a clause to arbitrate disputes as part of the terms and conditions in the agreements when opening an account.
- **Issue:** Should the court support T-Mobile's forced arbitration clause? Did T-Mobile's negligence lead to the data breach?
- **Ruling:** The Court ruled that a settlement would be appropriate in this case, which resulted in a $350 million payout that will fund claims by class members, plaintiffs' legal fees, and administrative costs.
- **Observation:** If the named plaintiffs have opted out of the arbitration clause, it is possible for a settlement case to proceed.

(c) 2023 Lexeprint Inc. All Rights Reserved.



(c) 2023 Lexeprint Inc. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC